Viruses that leave victims red in the Facebook
Brad Stone

It used to be that computer viruses attacked only your hard drive. Now they attack your dignity.

Malicious programs are rampaging through Web sites like Facebook and Twitter, spreading themselves by taking over people's accounts and sending out messages to all of their friends and followers. The result is that people are inadvertently telling their co-workers and loved ones how to raise their I.Q.'s or make money instantly, or urging them to watch an awesome new video in which they star.

"I wonder what people are thinking of me right now?" said Matt Marquess, an employee at a public relations firm in San Francisco whose Twitter account was recently hijacked, showering his followers with messages that appeared to offer a $500 gift card to Victoria's Secret.

Mr. Marquess was clueless about the offers until a professional acquaintance asked him about them via e-mail. Confused, he logged in to his account and noticed he had been promoting lingerie for five days.

"No one had said anything to me," he said. "I thought, how long have I been Twittering about underwear?"

The humiliation sown by these attacks is just collateral damage. In most cases, the perpetrators are hoping to profit from the referral fees they get for directing people to sketchy e-commerce sites.

In other words, even the crooks are on social networks now — because millions of tightly connected potential victims are just waiting for them there.

Often the victims lose control of their accounts after clicking on a link "sent" by a friend. In other cases, the bad guys apparently scan for accounts with easily guessable passwords. (Mr. Marquess gamely concedes that his password at the time was "abc123.")

After discovering their accounts have been seized, victims typically renounce the unauthorized messages publicly, apologizing for inadvertently bombarding their friends. These messages — one might call them Tweets of shame — convey a distinct mix of guilt, regret and embarrassment.

"I have been hacked; taking evasive maneuvers. Much apology, my friends," wrote Rocky Barbanica, a producer for Rackspace Hosting, an Internet storage firm, in one such note.

Mr. Barbanica sent that out last month after realizing he had sent messages to 250 Twitter followers with a link and the sentence, "Are you in this picture?" If they clicked, their Twitter accounts were similarly commandeered.

"I took it personally, which I shouldn't have, but that's the natural feeling. It's insulting," he said.

Earlier malicious programs could also cause a similar measure of embarrassment if they spread themselves through a person's e-mail address book.

But those messages, traveling from computer to computer, were more likely to be stopped by antivirus or firewall software. On the Web, such measures offer little protection. (Although they are popularly referred to as viruses or worms, the new forms of Web-based malicious

programs do not technically fall into those categories, as they are not self-contained programs.)

Getting tangled up in a virus on a social network is also more painfully, and instantaneously, public. “Once it’s delivered to everyone in three seconds, the cat is out of the bag,” said Chet Wisniewski of Sophos, a Web security firm. “When people got viruses on their computers, or fell for scams at home, they were generally the only ones that knew about it and they cleaned it up themselves. It wasn’t broadcast to the whole world.”

Social networks have become prime targets of such programs’ creators for good reason, security experts say. People implicitly trust the messages they receive from friends, and are inclined to overlook the fact that, say, their cousin from Ohio is extremely unlikely to have caught them on a hidden webcam.

Sophos says that 21 percent of Web users report that they have been a target of malicious programs on social networks. Kaspersky Labs, a Russian security firm, says that on some days, one in 500 links on Twitter point to bad sites that can infect an inadequately protected computer with typical viruses that jam hard drives. Kaspersky says many more links are purely spam, frequently leading to dating sites that pay referral fees for traffic.

A worm that spread around Facebook recently featured a photo of a sparsely dressed woman and offered a link to “see more.” Adi Av, a computer developer in Ashkelon, Israel, encountered the image on the Facebook page of a friend he considered to be a reliable source of amusing Internet content.

A couple of clicks later, the image was posted on Mr. Av’s Facebook profile and sent to the “news feed” of his 350 friends.

“It’s an honest mistake,” he said. “The main embarrassment was from the possibility of other people getting into the same trouble from my profile page.”

Others confess to experiencing a more serious discomfiture.

“You feel like a total idiot,” said Jodi Chapman, who last month unwisely clicked on a Twitter message from a fellow vegan, suggesting that she take an online intelligence test.

Ms. Chapman, who sells environmentally friendly gifts with her husband, uses her Twitter account to communicate with thousands of her company’s customers. The hijacking “filled me with a sense of panic,” she said. “I was so worried that I had somehow tainted our company name by asking people to check their I.Q. scores.”

Social networking attacks do not spare the experts. Two weeks ago, Lee Rainie, director of the Pew Internet and American Life Project, a nonprofit research group, accidentally sent messages to dozens of his Twitter followers with a link and the line, “Hi, is this you? LOL.” He said a few people actually clicked.

“I’m worried that people will think I communicate this way,” Mr. Rainie said. “ ‘LOL,’ as my children would tell you, is not the style that I want to engage the world with.”

Fonte: New York Times, New York, Dec. 13th 2009, Internet, online.